Cisco − CNR and DHCP FAQs for Cable Environment

Table of Contents

CNR and DHCP FAQs for Cable Environment....1
Questions....1
Introduction....1
Q. How do I access CNR remotely?....1
Q. How do I access CNR remotely if the CNR server is behind a firewall?....2
Q. What is a policy in CNR and how do I configure policies?....2
Q. What is a scope in CNR and how do I configure it?....3
Q. How do I configure Client Class Processing via CNR's GUI?....4
Q. How to Calculate the Hexadecimal Value for DHCP Option 2 (time offset)....5
Q. How does the CMTS know the difference between PCs and cable modems?....5
Q. Why is it that cable relay−agent−option does not work in 12.0 code?....6
Related Information....6

CNR and DHCP FAQs for Cable Environment

Questions

Introduction
How do I access CNR remotely?
How do I access CNR remotely if the CNR server is behind a firewall?
What is a policy in CNR and how do I configure policies?
What is a scope in CNR and how do I configure it?
How do I configure Client Class Processing via CNR's GUI?
How to Calculate the Hexadecimal Value for DHCP Option 2 (time offset)
How does the CMTS know the difference between PCs and cable modems?
Why is it that cable relay−agent−option does not work in 12.0 code?
Related Information

Introduction

- The first six Q & A pairs cover **CNR** .
- The last two Q & A pairs cover **DHCP**.

Q. How do I access CNR remotely?

If you are running CNR GUI remotely on your PC with Windows 95 or NT you can connect to the server by adding a cluster and typing in the IP address and passwords or the CNR server. This will connect you to the server that provides DNS and/or DHCP services. Remember though, that this method requires that the CNR GUI be located on the remote client.

1. Select **Admin**.
2. Click the **List of Clusters** icon.
3. In the cluster dialogue box, click the **Add Cluster** button.
4. In the **Add Cluster** dialogue box, enter the cluster name or database hostname.
5. Select **Connect to this cluster** check box. Click **OK**.
6. In the login for Cluster, put username and password. Click **OK**.

If you are trying to access CNR from a SUN workstation where the CNR GUI does not reside, do the following to open the GUI and connect to the CNR server:

1. Do an **nslookup** on your SUN station to find out your address.
2. Open an X−term and set up your display by typing **xhost +** to allow connections to your SUN workstation. After you type this command you will get the following message: "access control disabled, clients can connect from any host"
3. Telnet to the server.
4. Enter login and password.
5. Type **setenv TERM xterm**.
6. Type **setenv DISPLAY <your ip address>:0.0**
7. When you are at the UNIX prompt **#** type: **cd /opt/nwreg2/usrbin/ntwkreg &**
8. Network Registrar will display the Server Manager.
9. Select **Admin**
10. Click on the **List of Clusters** icon.
11. In the cluster dialogue box, click the **Add Cluster** button.

12. In the **Add Cluster** dialogue box, enter the cluster name or database hostname.
13. Select **Connect to this cluster** check box. Click **OK**.
14. In the login for Cluster, put username and password. Click **OK**.

Q. How do I access CNR remotely if the CNR server is behind a firewall?

If the server is to be managed remotely, perhaps being monitored round−the−clock by a network operation team, open the user interface ports. For getting the CNR GUI/CLI to open thought the firewall open UDP ports 2785 and 2786. The first port is for the outgoing and the second for the incoming data. Additionally, the well known ports for DHCP are 67 and 68, for DHCP failover the port is 647, for DNS use port 53. Other ports that can be opened are 389 for LDAP and 69 for TFTP.

Q. What is a policy in CNR and how do I configure policies?

A policy is a set of options that allow you to group lease times and other configuration parameters that a DHCP server assigns to a client. These parameters are called DHCP options. Policies are useful if you have more than one scope at your site. You can create a policy that applies to all the scopes on the current server, or create a policy for a selected scope. Policies are a convenient way of ensuring that your DHCP server supplies all the correct options for scopes, and frees you from the task of specifying the information separately per scope.

To create a policy do the following:

1. Open up CNR GUI. From the Server Manager window, select the DHCP server for which you want to create a policy. IF this is the first time you are doing this you will click on DHCP@localhost server icon.
2. Click the **Show Properties** toolbar button to display the DHCP Server Properties dialog box.
3. Click the **Policies** tab.
4. Click the **New...** button to display the New Policy dialog box.
5. In the **Name** field, enter the policy's name.
6. Do one of the following in the **Copy from** field:

    ◊ Select an existing policy to use as the starting point for the new policy.
    ◊ Select default to create a policy from scratch.
7. Click **OK**.
8. On the Policies tab, choose whether you want the leases to be permanent (never expire) or whether you want leases to have a duration. If you want them to be permanent, check out the box "Leases are permanent" and skip to step 11, otherwise continue to step 9.
9. Set the duration of the lease, for example seven days. The default value is seven days.
10. Set the duration of the grace period, for example four days. The lease grace period is the length of time that the lease is retained in the DHCP server's database after it has expired. The grace period protects a client's lease in cases where the client and server are in different time zones, the computer clocks are not synchronized, or the client was not on the network when the lease expired. The default value is five minutes.
11. Click **Edit options...**. The minimum options that you need to configure in a Cable Network environment are:

- ◊ **dhcp−lease−time**: This is the lease time in seconds. For 7 days = (60 sec/min)*(60min/hr)*(24hrs/day)*(7days) = 604800 sec.
- ◊ **tftp−server**: The IP address of the TFTP server (in this case it is the IP address of the server where CNR lives)
- ◊ **time−offset**: The number of seconds from GMT time. PTS time = −8hr = (3600 sec/hr)*(8hrs) = −28800. See the time offset conversion table.
- ◊ **time−server**: This is the IP address of the Time of Day (ToD) server.
- ◊ **packet−siaddr**: The IP address of the TFTP server.
- ◊ **routers**: This is the primary IP address of the cable interface on the CMTS.
- ◊ **packet−filename**: This is the name of the DOCSIS configuration file that will be used for the policy.

12. To configure these options go to the Available column, select the option you want to add in the following way:

    - ◊ To get to **tftp−server** scroll up the available window and click on **+** next to **Servers** option group, then click on **tftp−server** and click on the **add** > > > button and enter the value in the **Option value(s)** field.
    - ◊ To get to **time−offset** scroll down to **time−offset** and click the **add** > > > button. In the **Option value(s)** field type the correct value in seconds.
    - ◊ To get to **timeserver** scroll down and click on **timeserver**. Click the **add** >>> button. In the "Option value(s)" field type the correct ip address.
    - ◊ To get **packet−siaddr** scroll up and click on the **+** next to **DHCP Packet Fields** select **packet−siaddr** and click the **add** >>> button. In the **Option value(s)** field type the correct ip address.
    - ◊ To get to **routers** scroll up and click on **+** next to **Basic c** and select **routers**. Click the **add** >>> button and enter the corresponding ip address in the **Option value(s)** field.
    - ◊ To get to **packet−file−name** go to **DHCP Packet Fields** and select **packet−file−name**. Click the **add** >>> button and enter the name of the DOCSIS config file in the **Option value(s)** field. Check the **Always send to DHCP clients** check−box.

13. Click the **OK** button at the bottom of the **Edit Options** window when you are done.
14. Click **Yes** in the **Network Registrar** window that will pop up asking to commit the changes.
15. Click on each entry on the **active** field of the **DHCP@localhost Properties** window and verify the value in the **Value(s)** field. If you made a mistake, click on the **Edit Options...** button and change the mistaken option.
16. Click the **Close** button of the **DHCP@localhost Properties** window.

Q. What is a scope in CNR and how do I configure it?

A scope contains a set of IP addresses for part of or an entire subnet, and an associated policy that tells DHCP how to operate on these addresses. You must define at least one scope for each subnet on which you want a DHCP server to supply IP addresses to DHCP clients. Note that you can have more than one scope per subnet, and you can combine secondary subnets as well. For more information, see Using Network Registrar or the online help.

To create a scope do the following:

1. From the **Server Manager** window, select the DHCP server to which you want to add a scope.
2. Click the **Add** toolbar button to display the **Add Scope** dialog box.

3. In the **Name** field, enter the name of the scope.
4. In the **Policy** field, do one of the following:

    ◊ Click the arrows to select the policy you want applied to this scope.
    ◊ Click the View policy button to create a new policy or edit an existing one.
5. In the **Network number** field, enter the server's network number. In cable network environment, this network number corresponds to the primary ip address on the cable interface in the CMTS.
6. In the **Subnet mask** field, enter the subnet mask.
7. In the **Start/End Address** columns, specify the scope address range by typing a series of single addresses and/or address ranges. Make sure that none of those addresses are assigned to the cable interfaces on the CMTS.
8. Click **OK**.

Q. How do I configure Client Class Processing via CNR's GUI?

To configure client class processing, you have to first create the policies and then configure scopes assigning the correspondent policy to the scope. Once you have done these two steps, you can follow the procedure below.

First, enable client−class processing for the DHCP server and its scopes.

1. In the **Server Manager** window, double−click the DHCP server.
2. In the **DHCP Server Properties** dialog box, click the **Scope Selection Tags** tab.
3. Click the **Enable client−class processing** check box. There are initially no scope selection tags defined in the **Scope selection tags currently defined for this DHCP server are listed below** box.

Second, add Scope selection tags in the following way:

1. On the **Scope Selection Tags** tab of the "DHCP Server Properties" dialog box, enter a name in the field at the bottom of the dialog box. To identify it as a tag, it is best to prefix it accordingly; for example, "tagCableModemUnprov" for the unprovisioned cable modems to "tagCableModem" for the provisioned cable modems. If not satisfied with your entry, click the Clear button to clear the field.
2. Click the **Add** button. The name appears under in the table in the middle of the dialog box. Note that you must click **Add**. If you click OK, the dialog box closes without the entry being added. Using the GUI, you can only add selection tags, you cannot delete them.
3. Add more tags in the same way. If you change your mind about your entries, click Cancel.
4. If you are sure of your entries, click **OK**.
5. Reload the DHCP server.

Third, Define Client Classes:

1. In the **DHCP Server Properties** dialog box for the appropriate server, click the **Client−Classes** tab.
2. Click the **Add** button to open the **Add Client−Class** dialog box.
3. Enter in the **Client−Class** field the name of the client−class. This should clearly identify the intent of the client−class, such as CableModem.
4. In the **Host Name** field, enter a host name.
5. In the **Policy Name field**, select the "DHCP policy" that is appropriate for the client−class, such as policyCableModem. To leave the policy name unspecified,

select **<Not Specified >**

6. In the **Policy Name field**, select the **DHCP policy** that is appropriate for the client−class, such as policyCableModem. To leave the policy name unspecified, select **<Not Specified >**
7. As a final step in this dialog box, add a comment or keyword in the **User Defined String** field. You can use this to index, sort, or search for the client−classes.
8. Click Apply to continue adding client−classes in the same way, or OK to finish. To remove a client−class from the DHCP Server Properties dialog box, select it, then click the Remove button.

Fourth, Associating a Selection Tag with a Scope.

1. In the **Server Manager** window, double−click the scope for which you want to apply selection tags for client−classes.
2. Click the **Selection Tags** tab from the **Scope Properties** window.
3. Click the **Edit Tags...** button. This opens the **Choose Scope Selection Tags** dialog box.
4. Select the check boxes for one or more of the scope selection tags defined for the server.
5. Click **OK**.
6. Click **OK** in the **Scope Properties** dialog box.
7. Reload the DHCP server.
8. Repeat these steps for each additional scope.

Q. How to Calculate the Hexadecimal Value for DHCP Option 2 (time offset)

If a cable modem were being used in a region that was GMT − 4 hours. In this case the negative value changes the procedure a little bit. The appropriate value would be calculated as follows: (Notice that 1hr = (60 minutes / hour) * (60 seconds / minute) = 3600 sec).

1. The number of seconds equivalent to − 4 hours = − 4 hours * (3600 second/hr) = − 14400 seconds.
2. In order to convert − 14400 to an unsigned 32 bit value we need to perform the following operation. (2^32 means 2 to the power of 32 = 4294967296). Then 2^32 − 14400 = 4294967296 − 14400 = 4294952896. We had to use this step because option 2 is 32 bits long.
3. Using a scientific calculator or a tool such as the calculator application included with Microsoft Windows we convert 4294952896 to a hexadecimal value. This turns out to be FFFFC7C0.
4. The value placed in the dhcp pool configuration now becomes option 2 hex FFFF.C7C0.

For more detailed information on how to do this read the document How to Calculate the Hexadecimal Value for DHCP Option 2 (time offset).

Q. How does the CMTS know the difference between PCs and cable modems?

In the past the we used to let Cisco Network Registrar (CNR) figure it out using DHCP option 82. The CMTS inserts option 82 into the DHCP discover packet. The cable modems Mac address is stuffed into this upstream discover packet and forwarded to the DHCP server. The DHCP server looks for a match of the "remote id" and "Mac address" that

making the request. If there is a match, it is a cable modem. If not, then this Mac address is another device like a PC. However, we also have a feature called **smart relay** on the cable interface which can figure out if incoming packets to the CMTS are a cable modem or a PC. See next question.

Q. Why is it that cable relay−agent−option does not work in 12.0 code?

Cisco uBR7200 series routers running Cisco IOS® Software Release 12.0 use the global configuration command **ip dhcp relay information option** to insert DHCP relay−agent option fields. (Previously, routers running Cisco IOS Software Release 11.3NA used the **cable relay−agent−option** command. However, 12.0SC code is an exception to the rule which also uses **cable relay−agent−option** because it was built off the Cisco IOS Software Release 11.3NA code with some added features like bundling). Therefore, if you are using Cisco IOS Software Release 12.0.7XR2 for concatenation, you should be able to configure the cable relay agent option using the **ip dhcp relay information option** command.

Related Information

- **Technical Support − Cisco Systems**

All contents are Copyright © 1992−2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.